Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

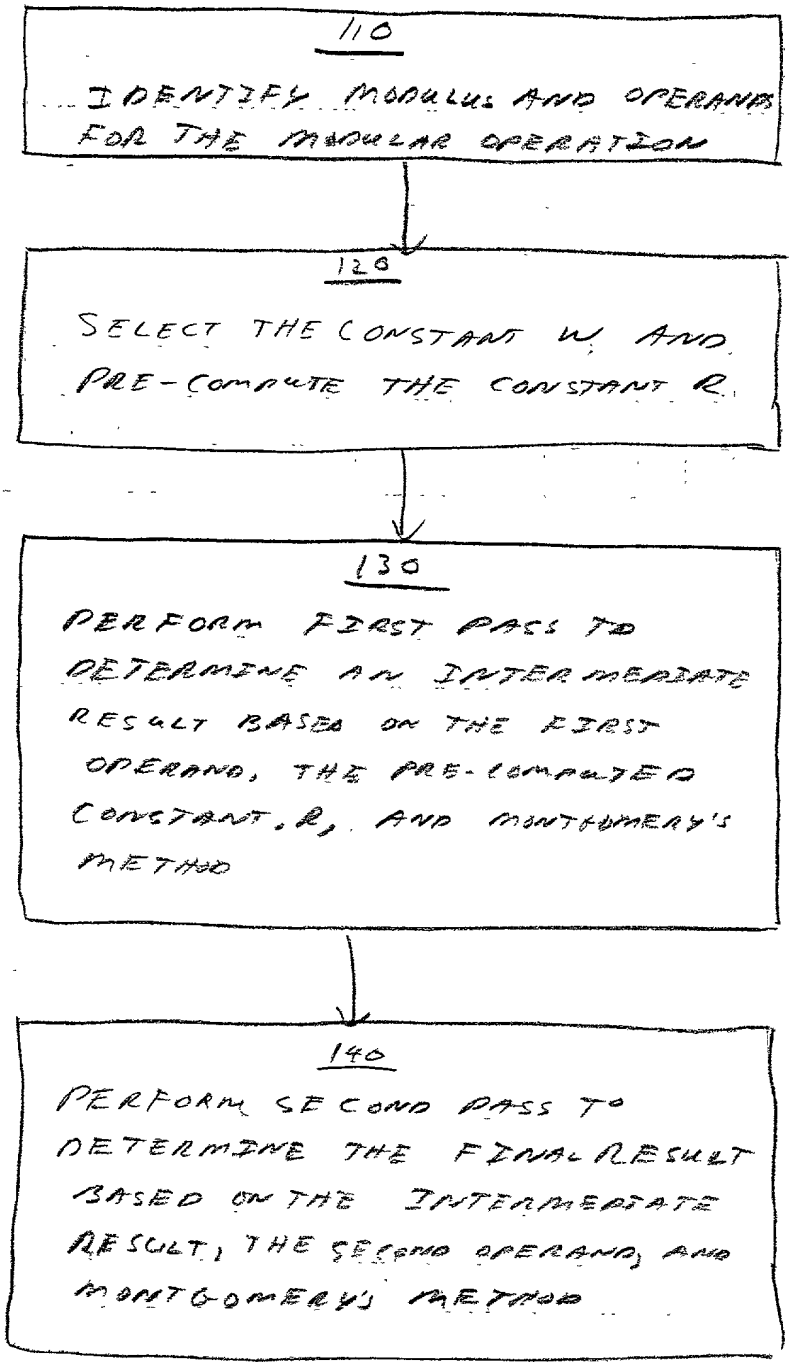


FIG 1

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

2/25

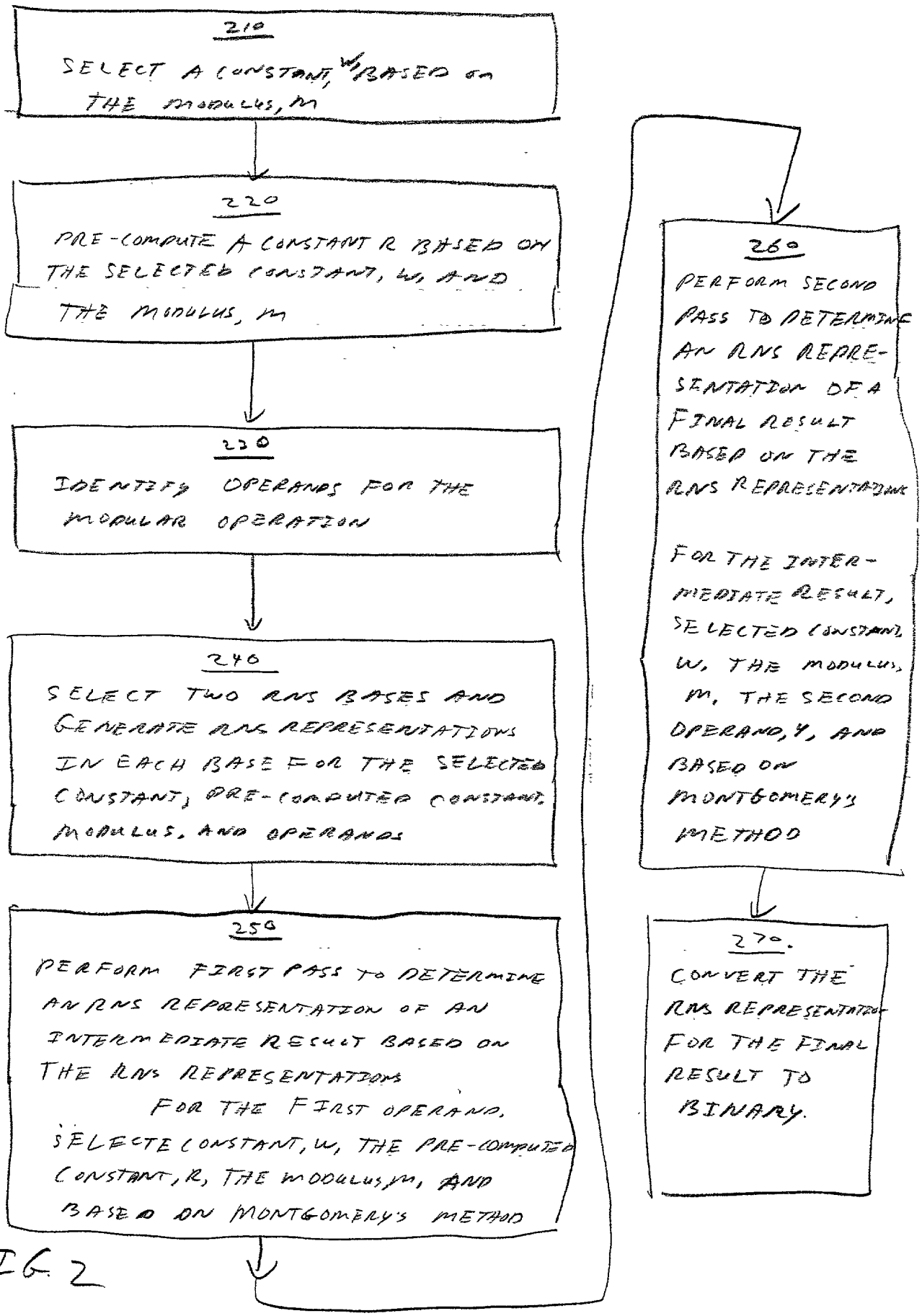


FIG 2

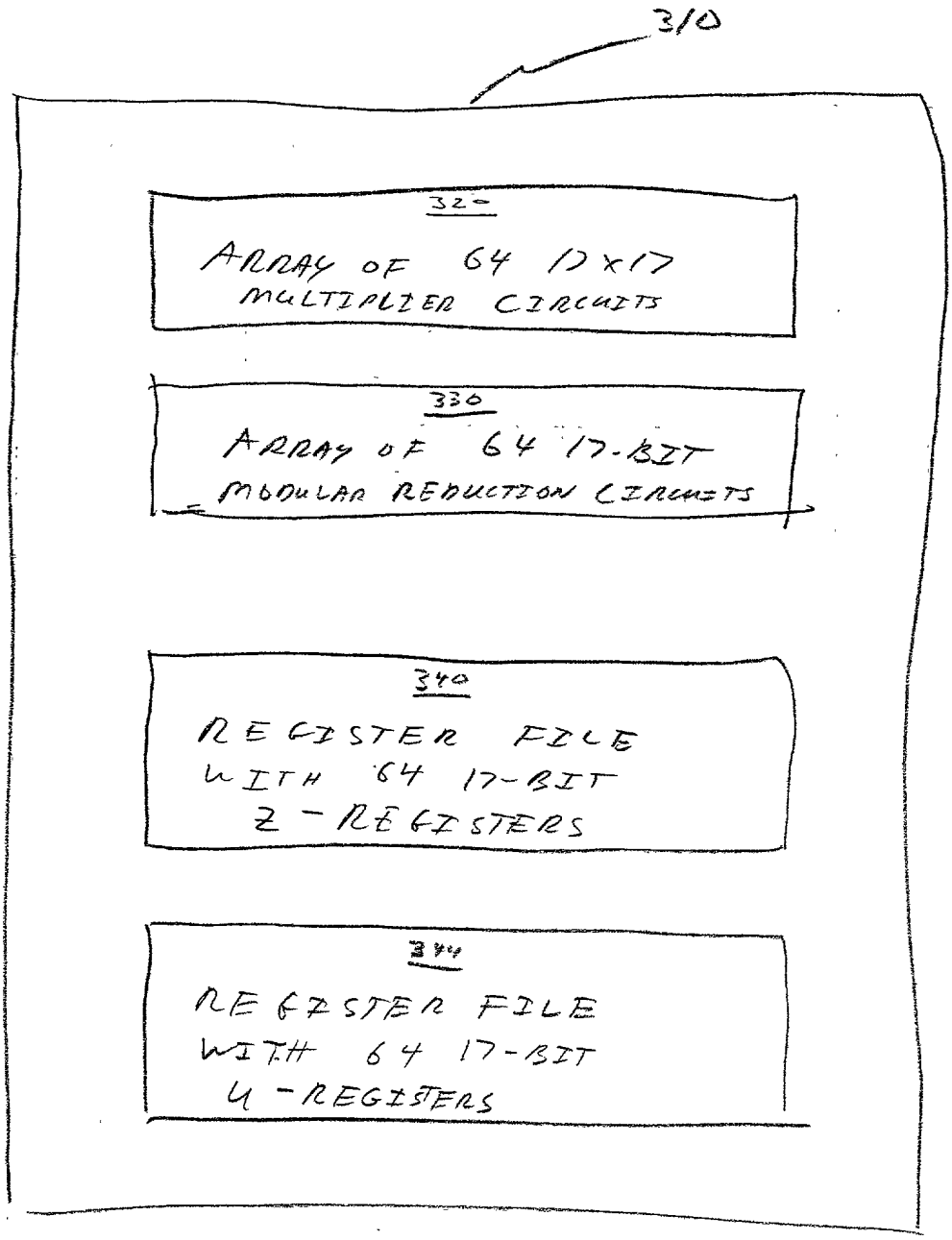


FIG. 3A

4/25

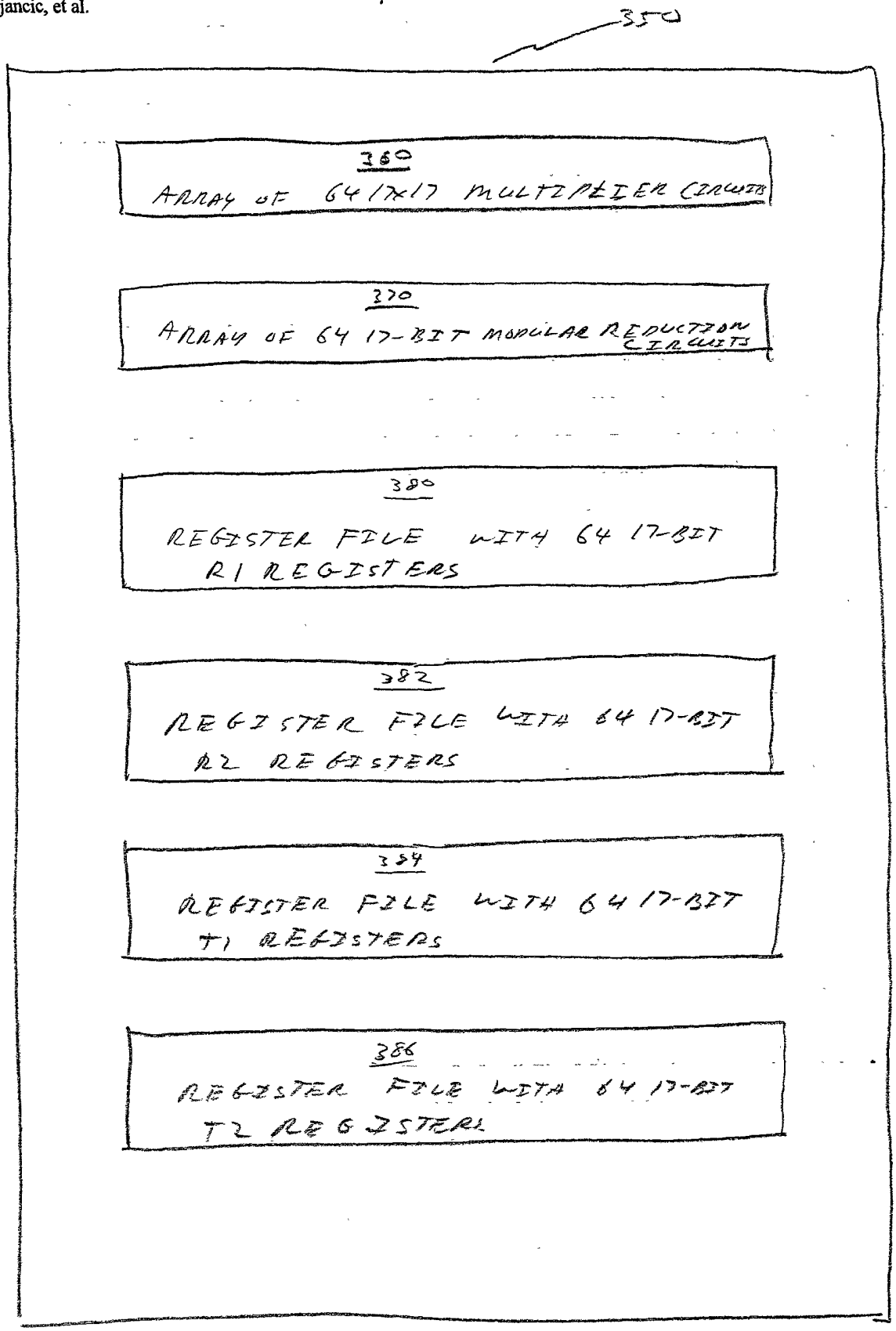

350
360
ARRAY OF 64 17x17 MULTIPLIER CIRCUITS
370
ARRAY OF 64 17-BIT MODULAR REDUCTION CIRCUITS
380
REGISTER FILE WITH 64 17-BIT R1 REGISTERS
382
REGISTER FILE WITH 64 17-BIT R2 REGISTERS
384
REGISTER FILE WITH 64 17-BIT T1 REGISTERS
386
REGISTER FILE WITH 64 17-BIT T2 REGISTERS

FIG 3B

5/25

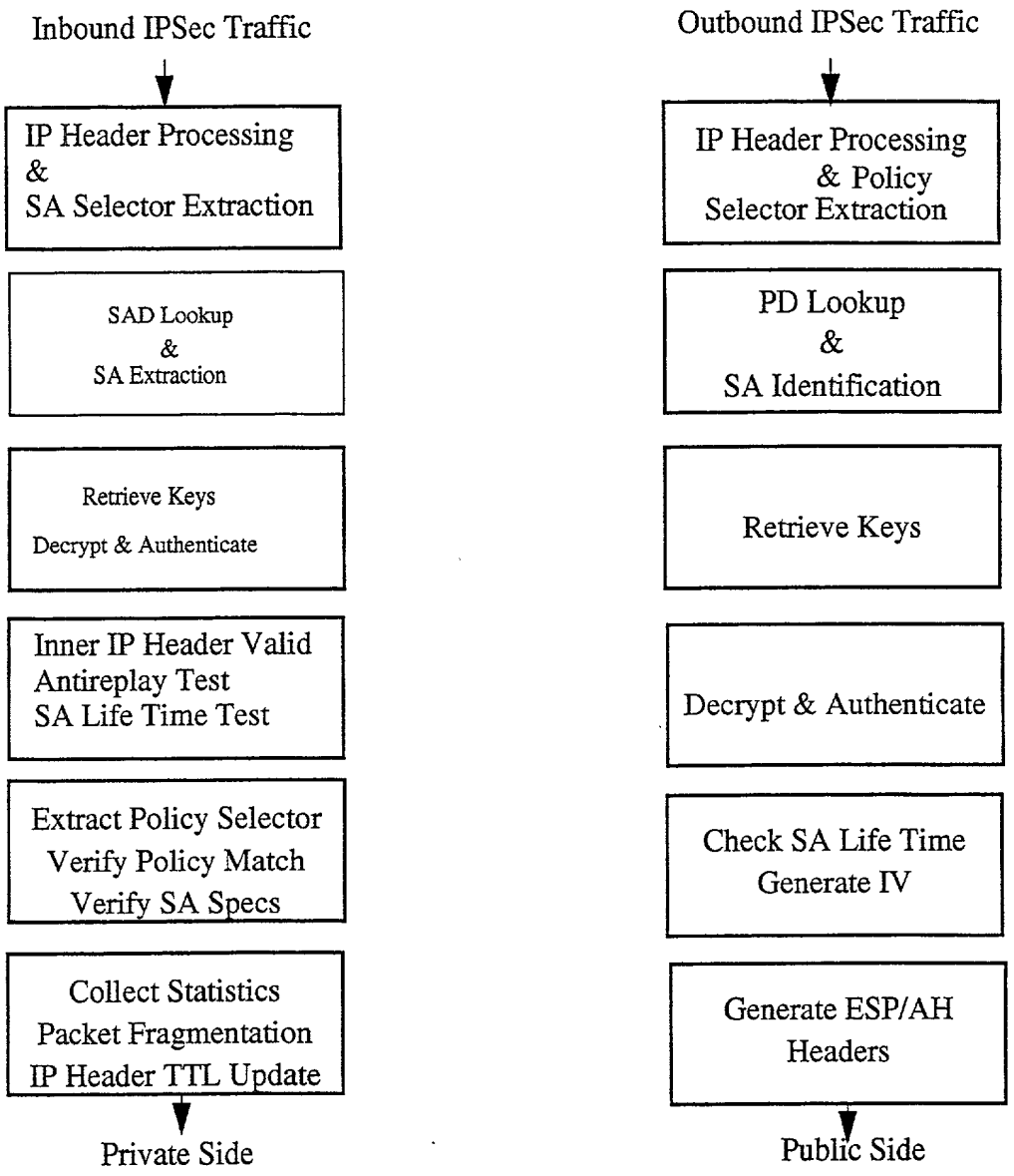


FIG. 4

6/25

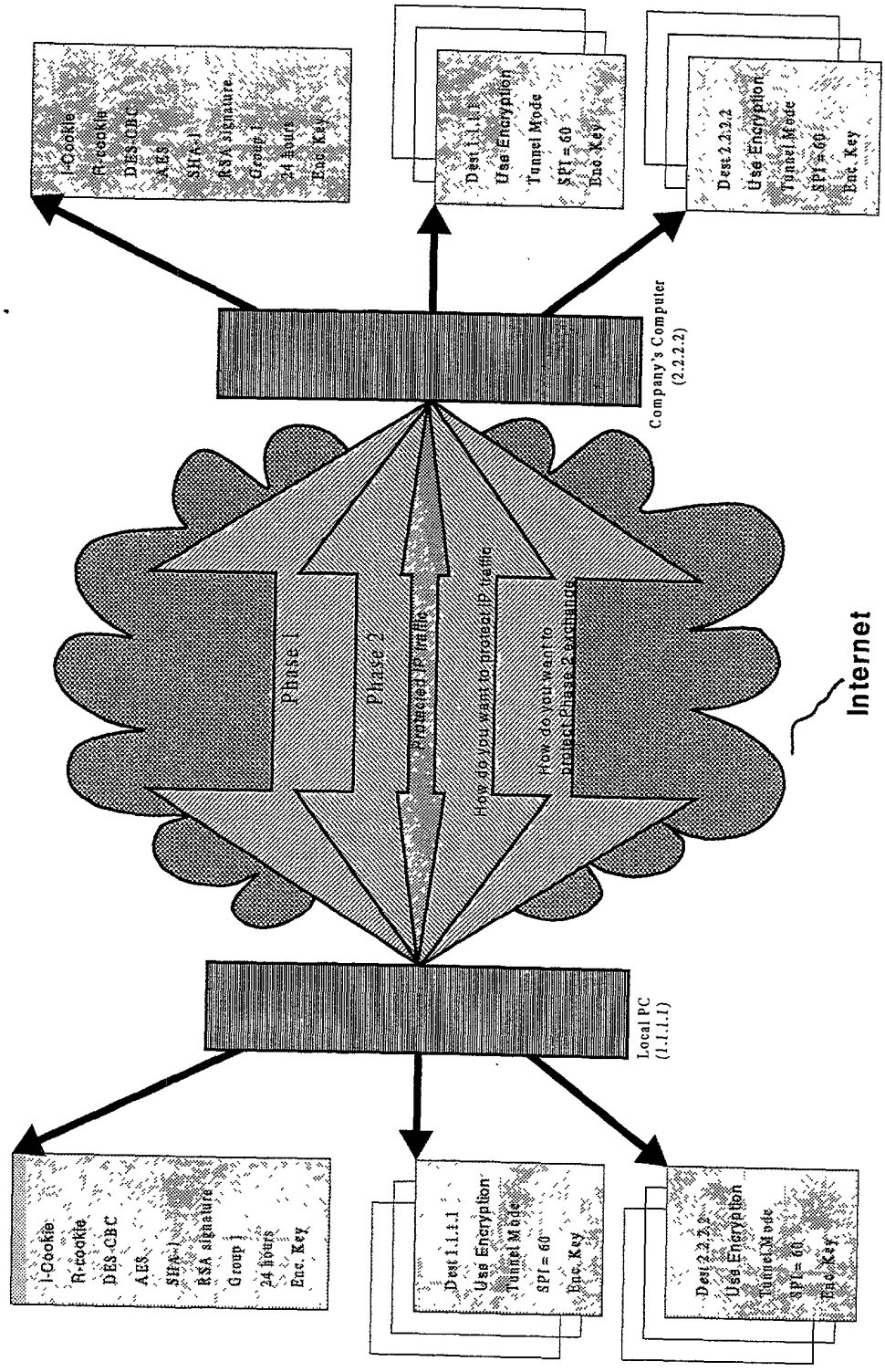

I-Cookie
R-cookie
DES-CBC
AES
SHA-1
RSA signature
Group 1
24 hours
Enc. Key
Dest 1.1.1.1
Use Encryption
Tunnel Mode
SPI = 60
End. Key
Dest 2.2.2.2
Use Encryption
Tunnel Mode
SPI = 60
Enc. Key
Company's Computer (2.2.2.2)
Phase 1
Phase 2
Protect IP traffic
How do you want to protect IP traffic
How do you want to protect Phase 2 exchange
Internet
Local PC (1.1.1.1)

FIG. 5

7/25

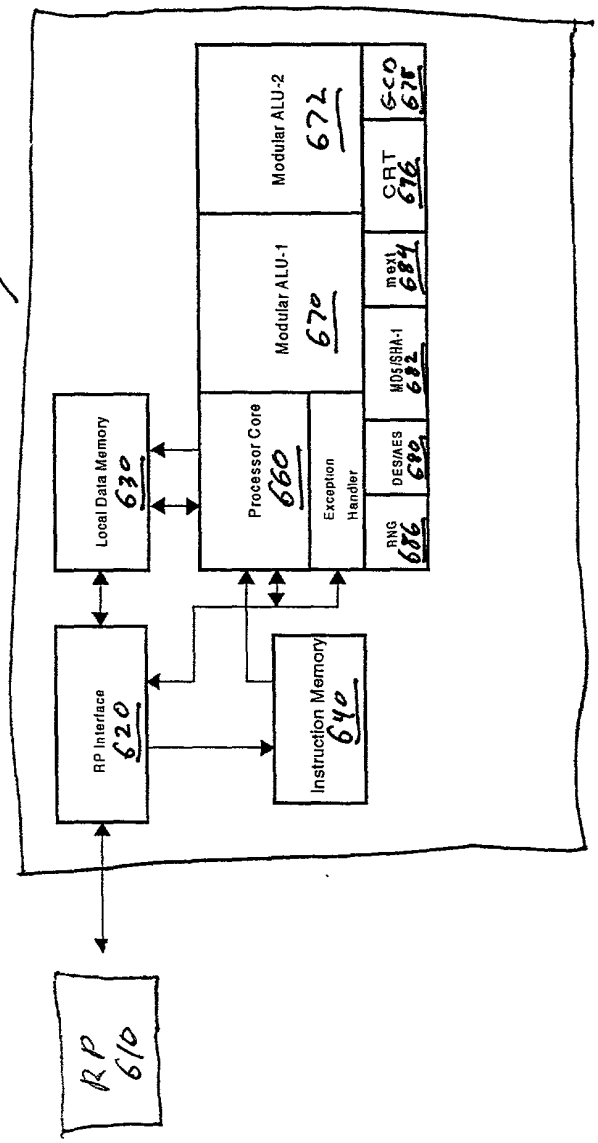
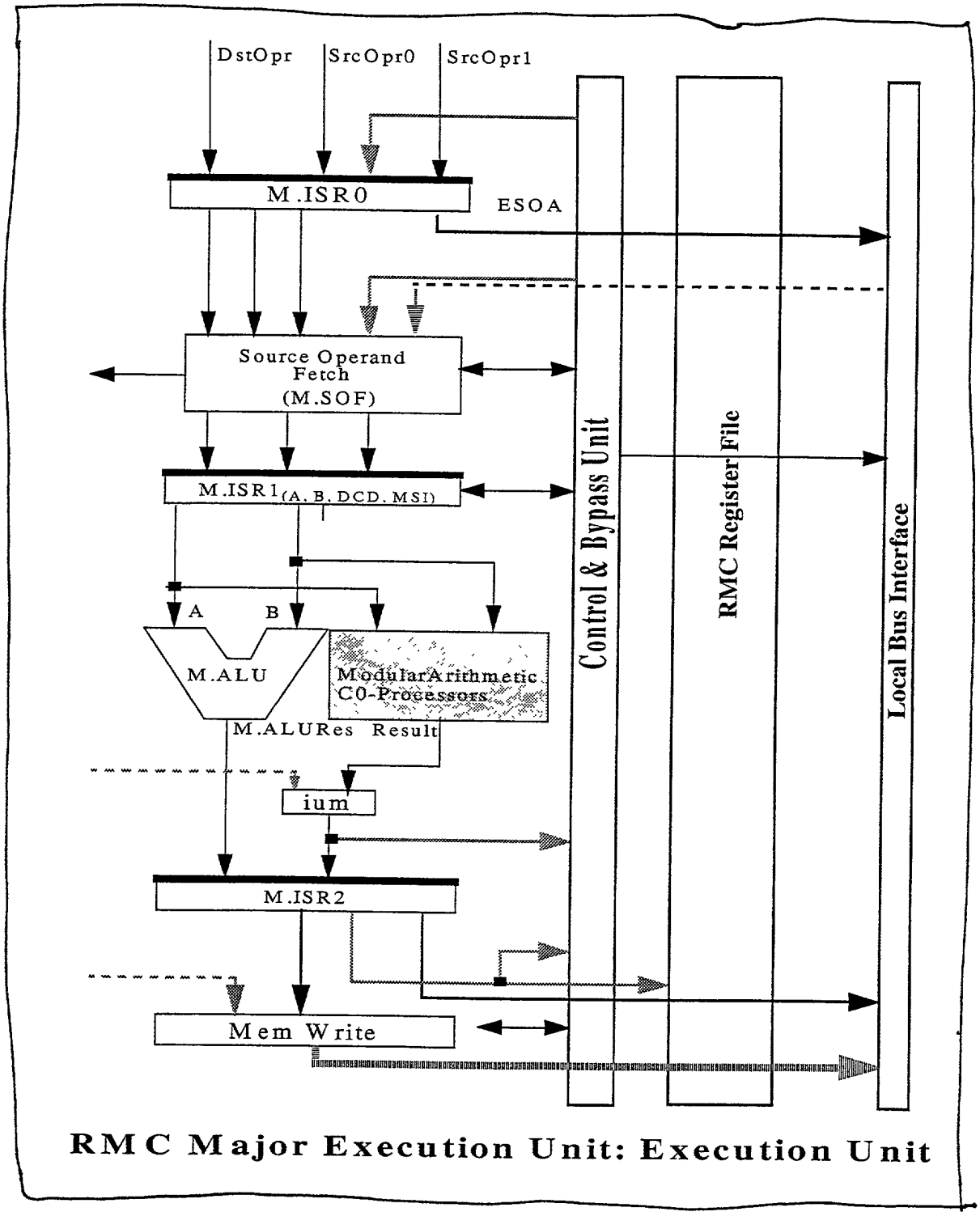

600
Modular ALU-2
672
GCO
675
CRT
676
mexl
684
Modular ALU-1
670
MD5/SHA-1
682
Local Data Memory
630
Processor Core
660
Exception Handler
DES/AES
680
RNG
686
RP Interface
620
Instruction Memory
640
RP
610

FIG. 6

8/25



RMC Major Execution Unit: Execution Unit

FIG. 7

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: Rectangular blocks on the same horizontal level overlap execution times.

⇐ - Source Overwrites Destination Register
® - Modular Multiplication with respect to w.
© - Modular Multiplication with respect to v.
∠ - RNS Conversion

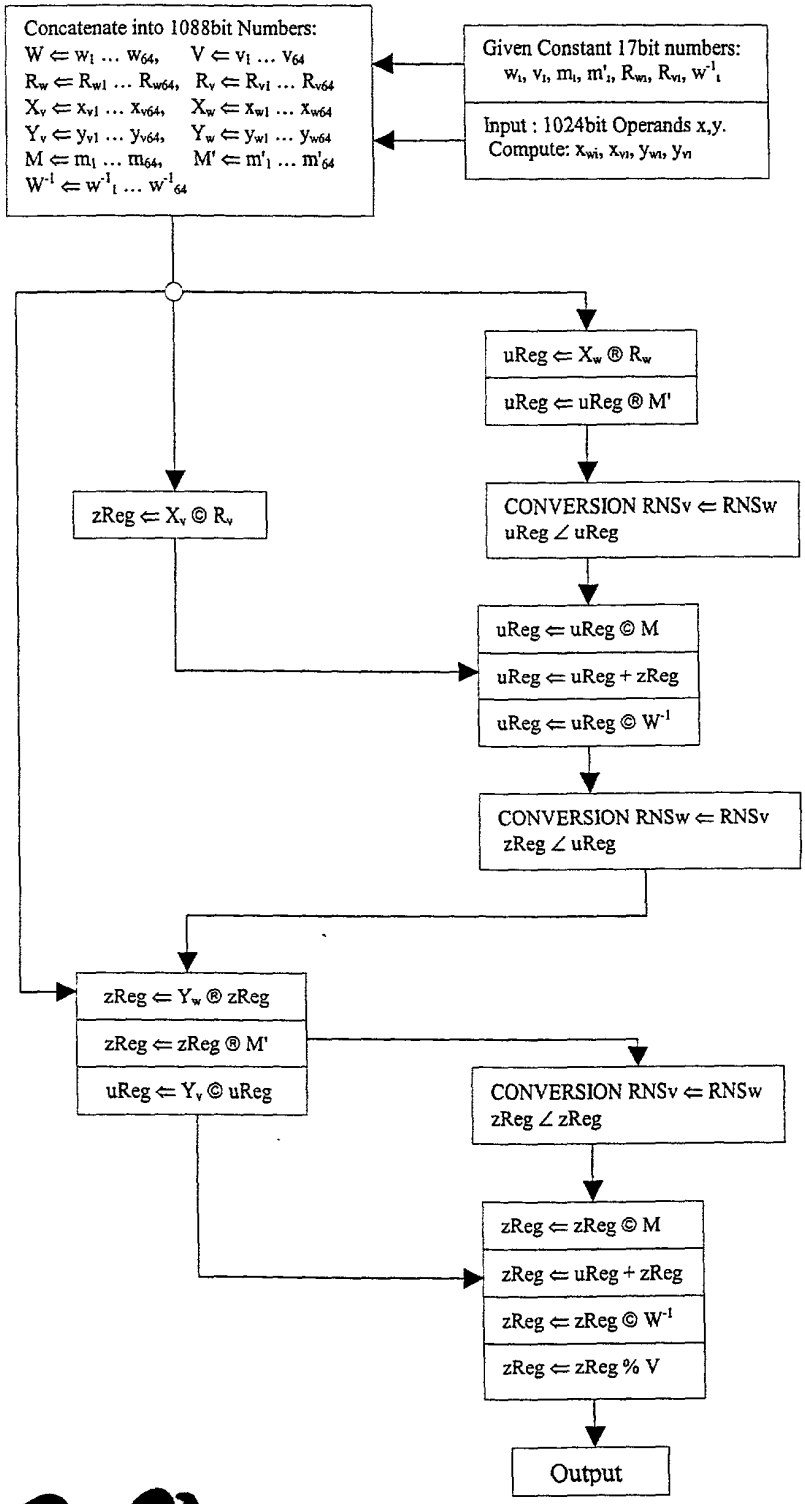


FIG. 8

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: All busses are 64x17 = 1088 bits wide.

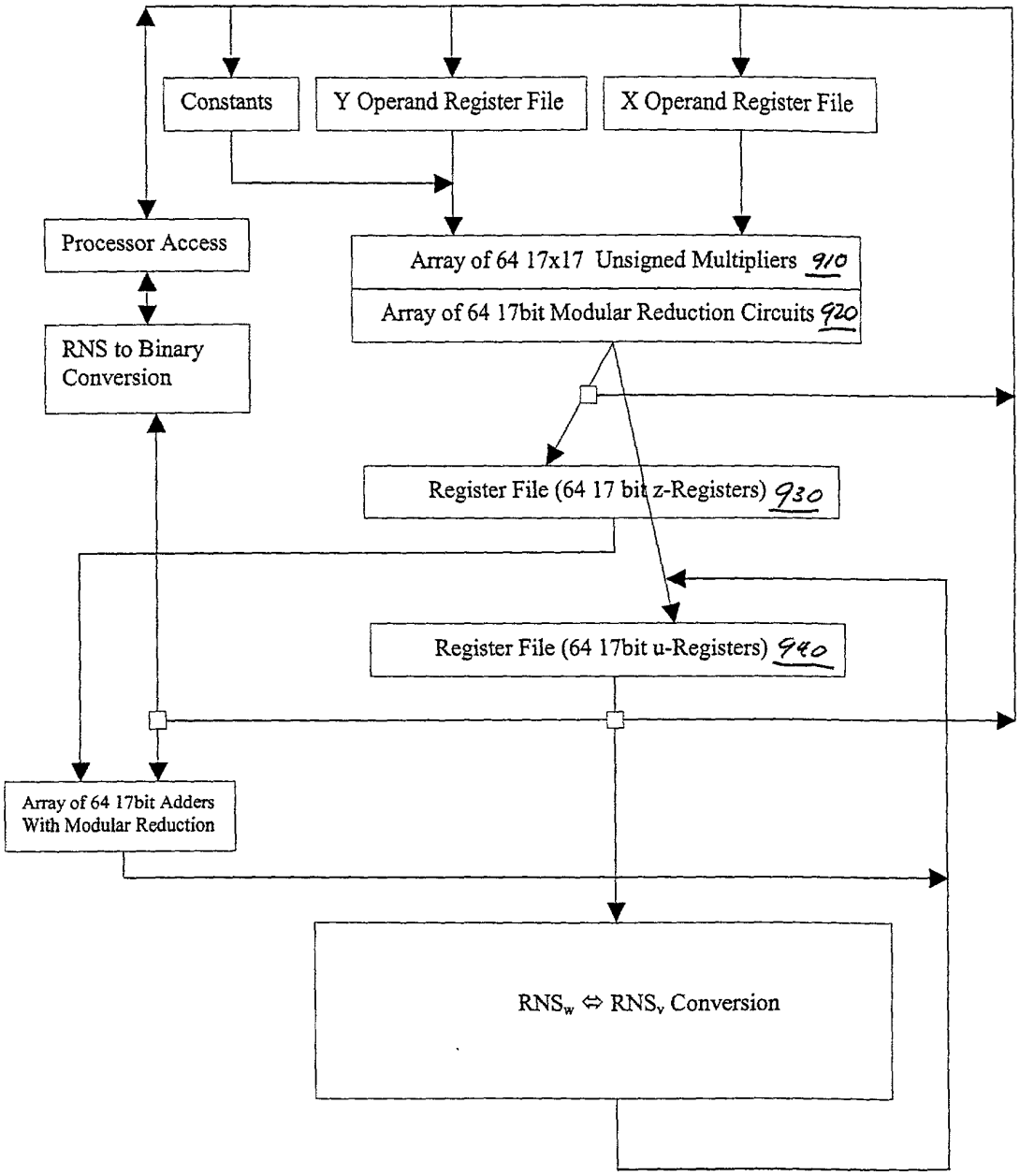


FIG. 9

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

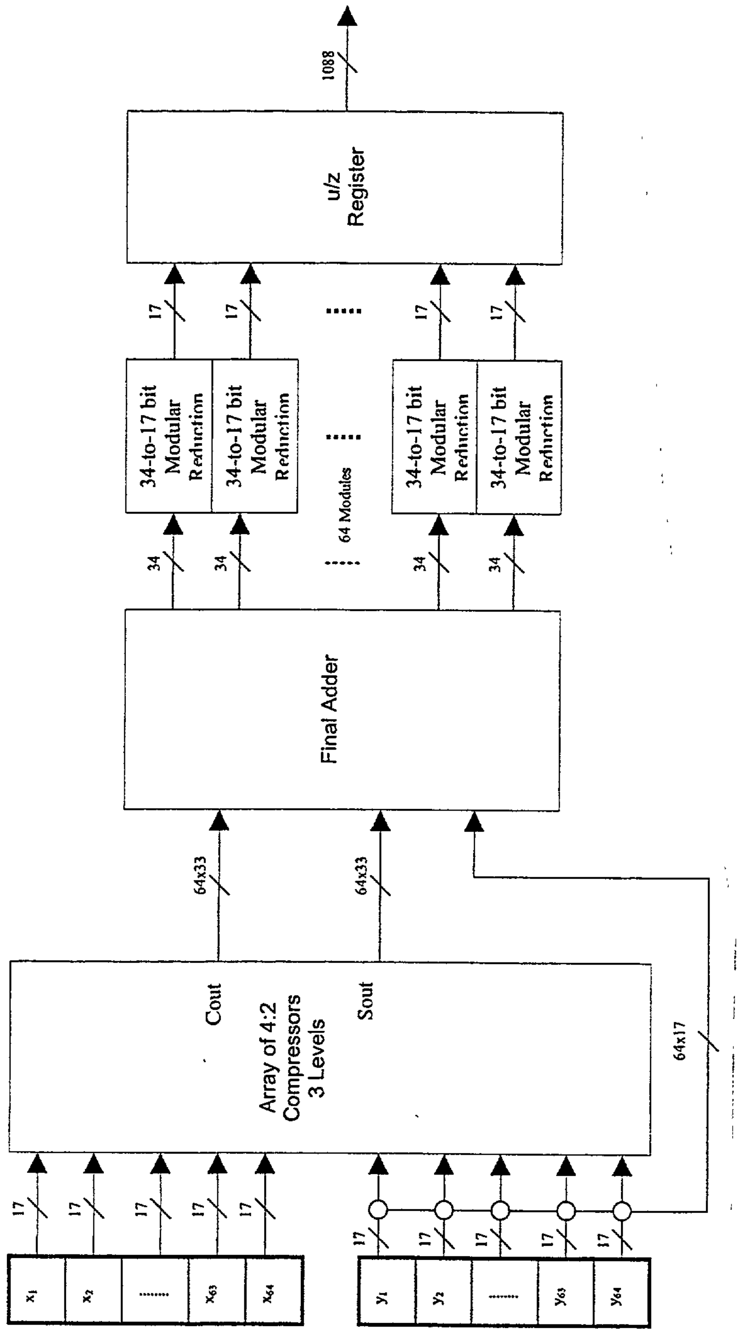


FIG. 10

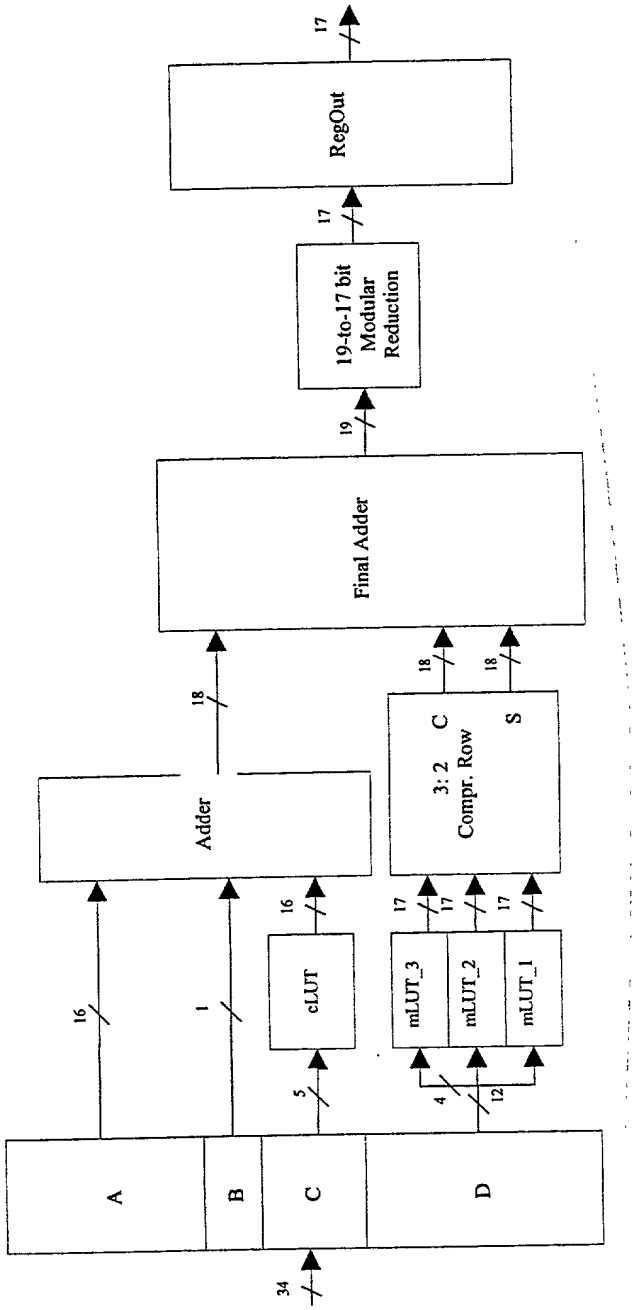

RegOut
17
19-to-17 bit Modular Reduction
17
19
Final Adder
18
18
Adder
3: 2 Compr. Row
C
S
16
1
16
cLUT
5
17
17
17
mLUT_3
mLUT_2
mLUT_1
4
12
A
B
C
D
34

FIG. 11

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: Rectangular blocks on the same horizontal level overlap execution times.

⇐ - Source Overwrites Destination Register
® - Modular Multiplication with respect to w.
© - Modular Multiplication with respect to v.
∠ - RNS Conversion

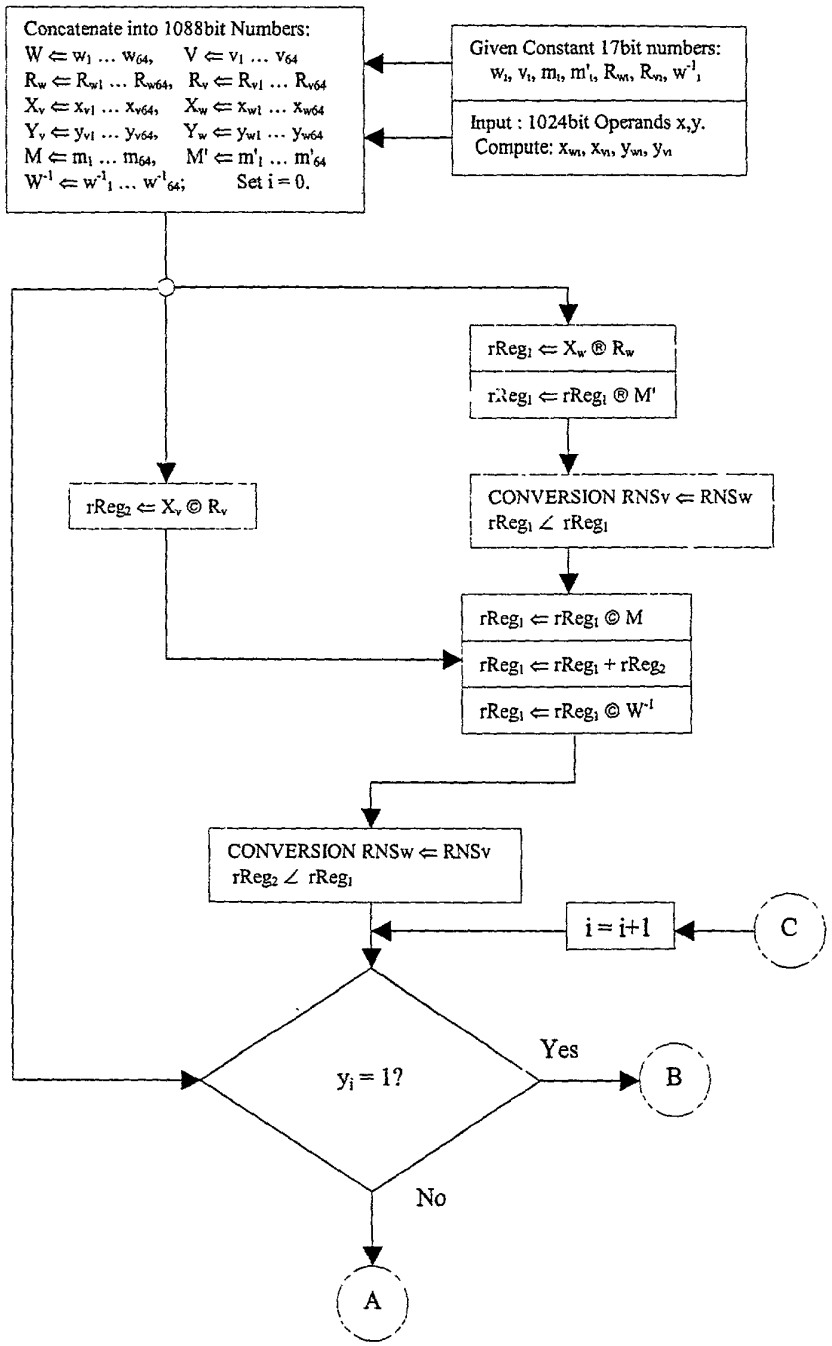


FIG. 12A

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

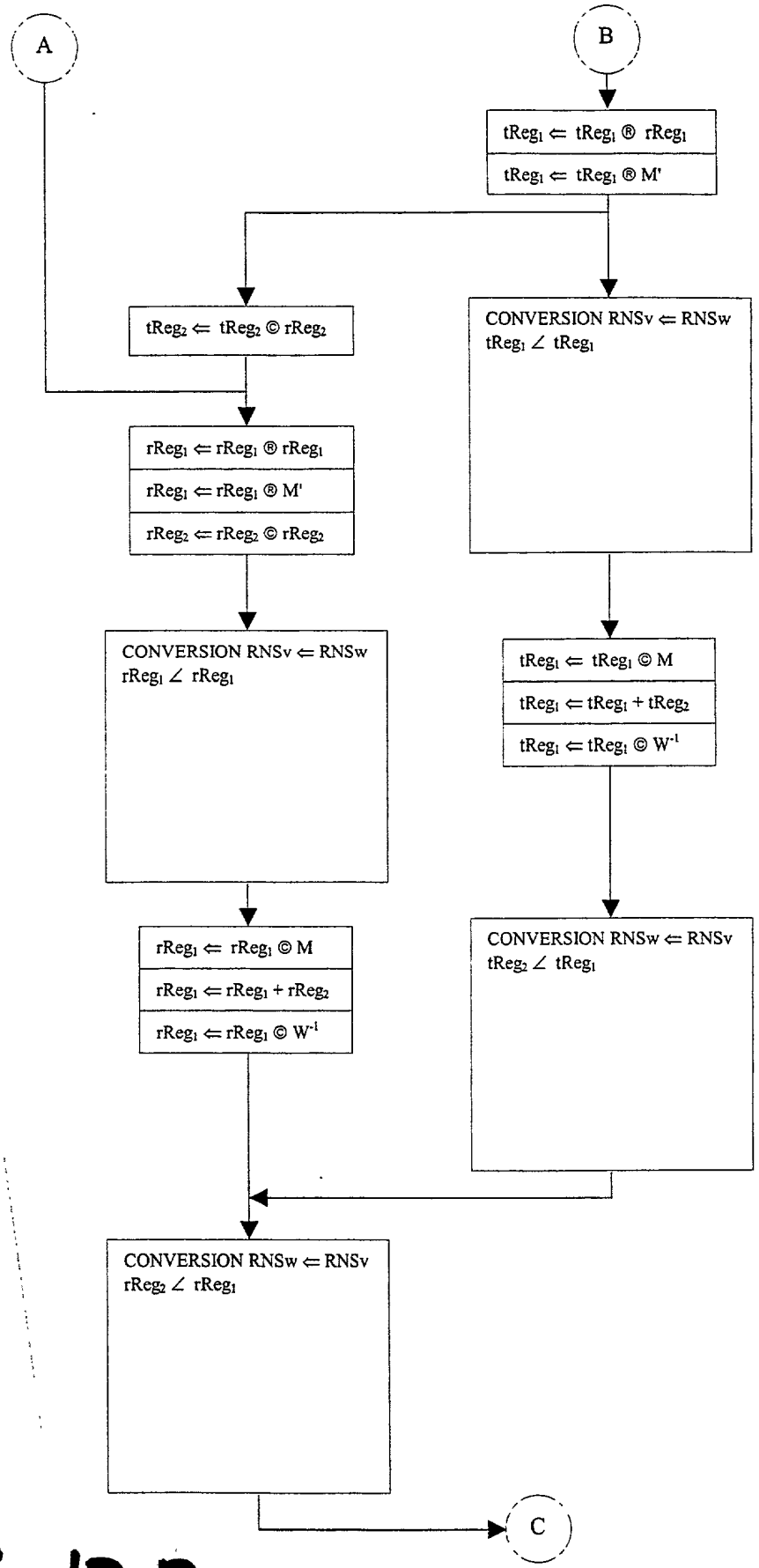


FIG. 12B

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: All busses are 64x17 = 1088 bits wide.

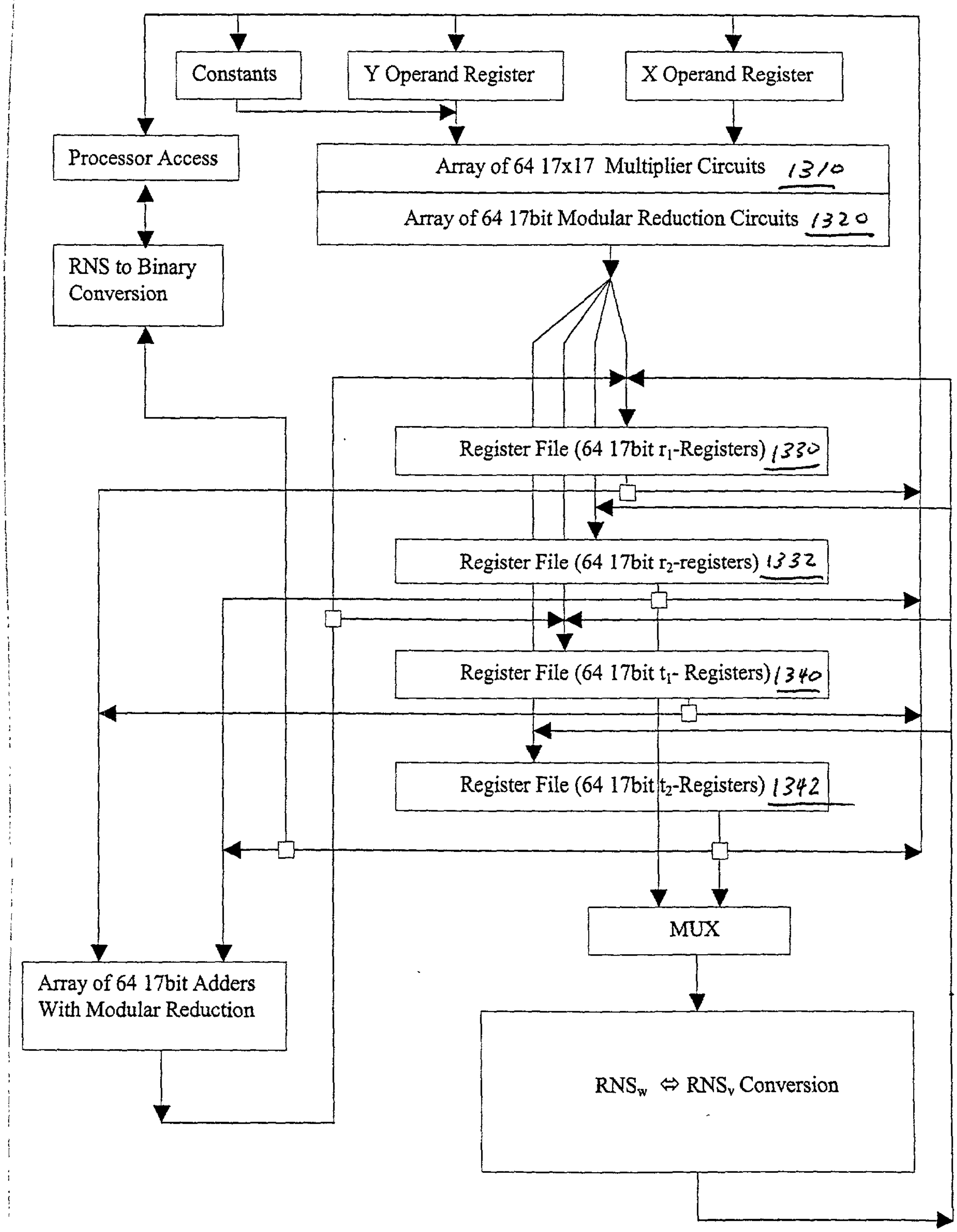


FIG. 13

16/25

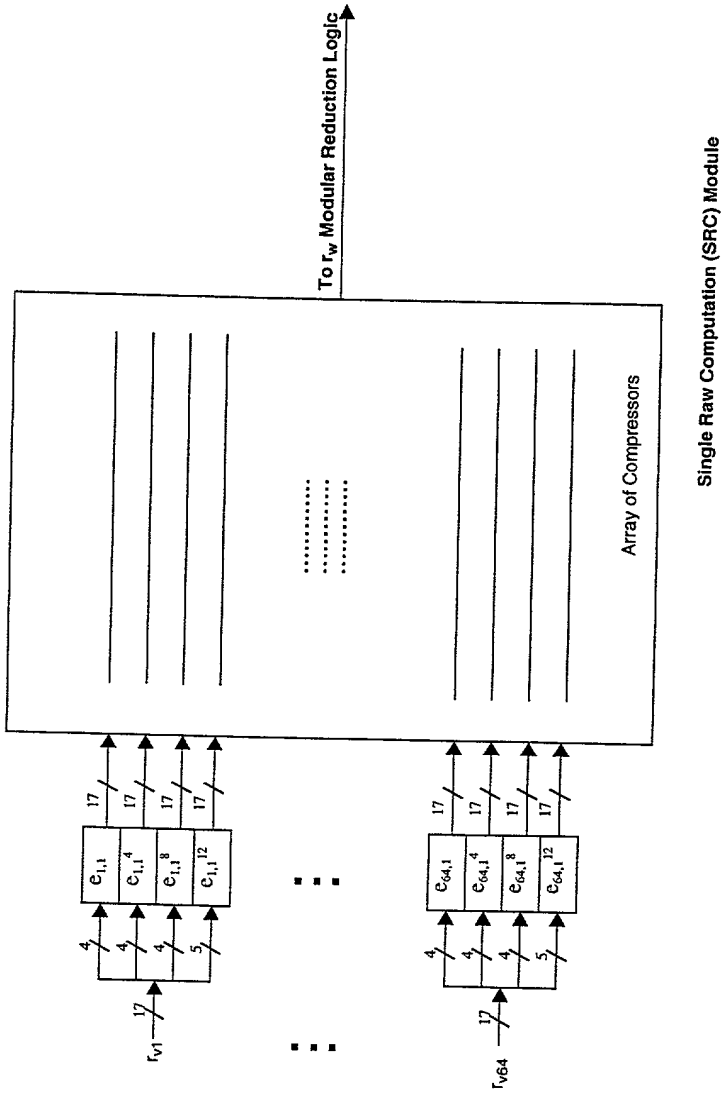

To r_w Modular Reduction Logic
Array of Compressors
Single Raw Computation (SRC) Module
$e_{1,1}$
$e_{1,1}^{4}$
$e_{1,1}^{8}$
$e_{1,1}^{12}$
$e_{64,1}$
$e_{64,1}^{4}$
$e_{64,1}^{8}$
$e_{64,1}^{12}$
17
4
5
r_{v1}
r_{v64}

FIG. 14

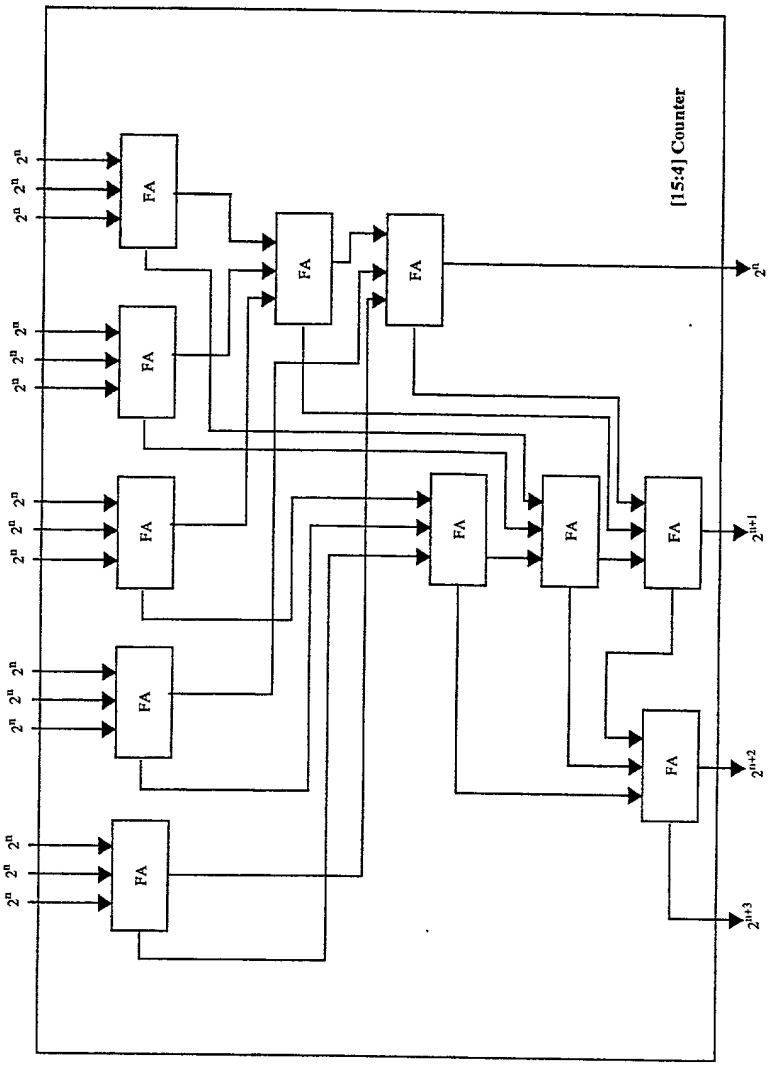


FIG. 15

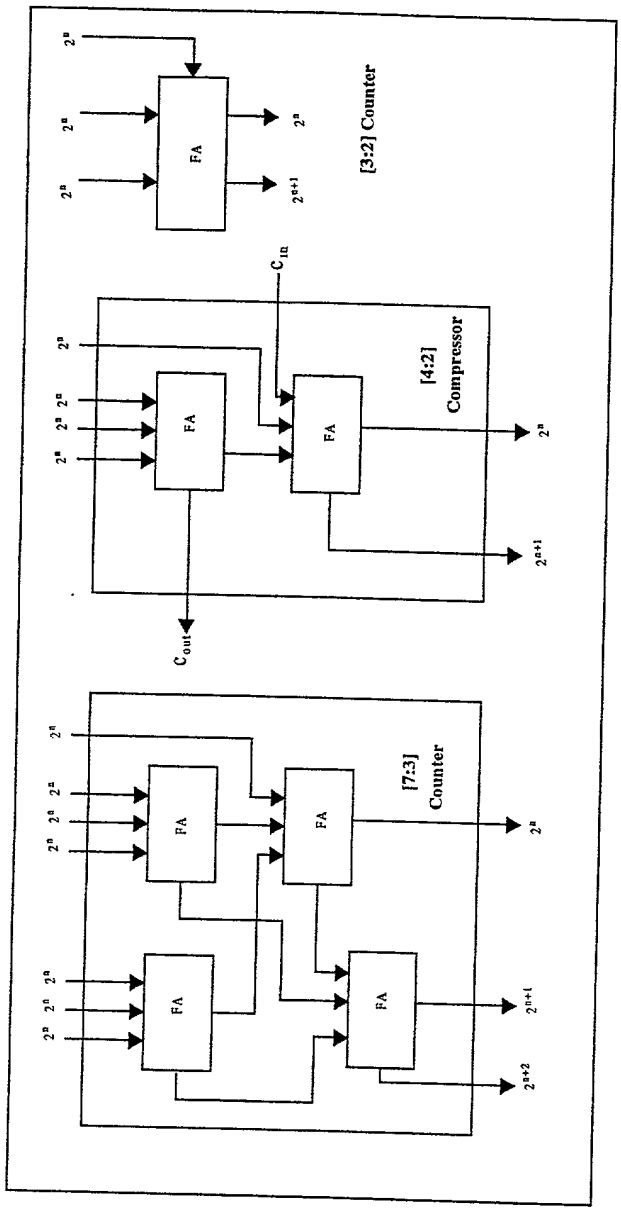


FIG. 16

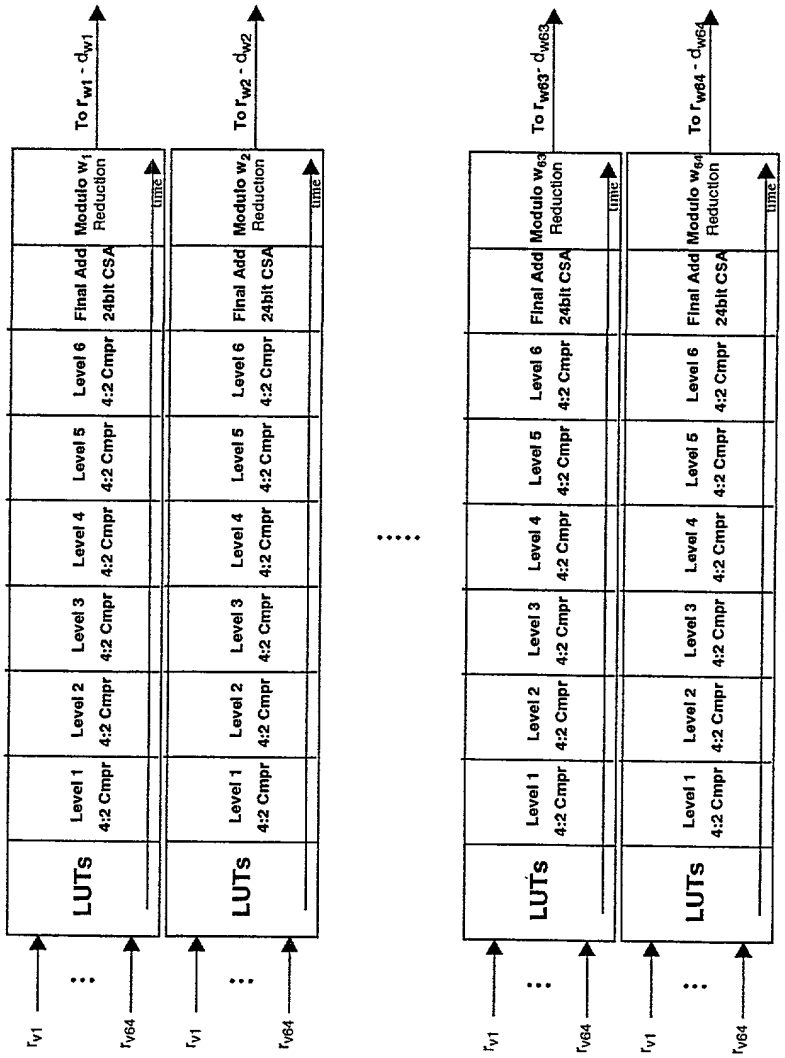

LUTs
Level 1 4:2 Cmpr
Level 2 4:2 Cmpr
Level 3 4:2 Cmpr
Level 4 4:2 Cmpr
Level 5 4:2 Cmpr
Level 6 4:2 Cmpr
Final Add 24bit CSA
Modulo w1 Reduction
Modulo w2 Reduction
Modulo w63 Reduction
Modulo w64 Reduction
time
To rw1 - dw1
To rw2 - dw2
To rw63 - dw63
To rw64 - dw64
rv1
rv64

FIG. 17

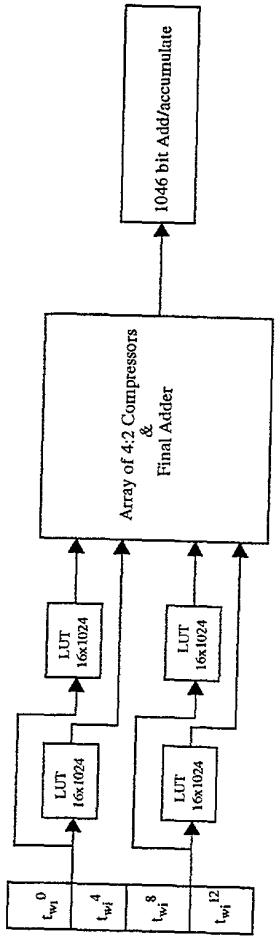

1046 bit Add/accumulate
Array of 4:2 Compressors & Final Adder
LUT 16x1024
LUT 16x1024
LUT 16x1024
LUT 16x1024
t_{wi}^{0}
t_{wi}^{4}
t_{wi}^{8}
t_{wi}^{12}

FIG. 18

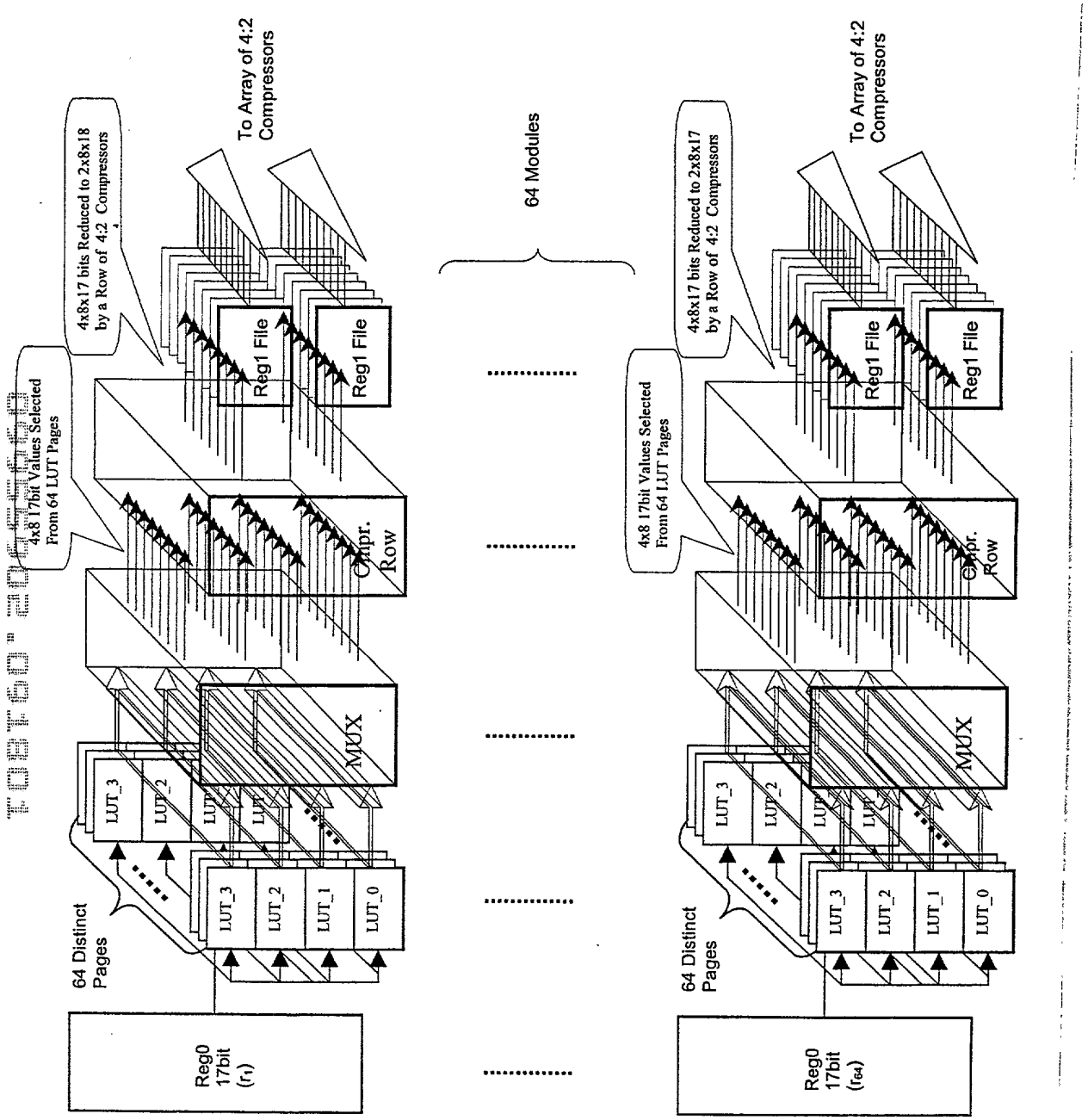

64 Modules
To Array of 4:2 Compressors
4x8x17 bits Reduced to 2x8x18 by a Row of 4:2 Compressors
4x8 17bit Values Selected From 64 LUT Pages
Reg1 File
Reg1 File
Compr. Row
MUX
LUT_3
LUT_2
LUT_1
LUT_0
64 Distinct Pages
Reg0 17bit (r_1)
To Array of 4:2 Compressors
4x8x17 bits Reduced to 2x8x17 by a Row of 4:2 Compressors
4x8 17bit Values Selected From 64 LUT Pages
Reg1 File
Reg1 File
Compr. Row
MUX
LUT_3
LUT_2
LUT_1
LUT_0
64 Distinct Pages
Reg0 17bit (r_{64})

FIG. 19

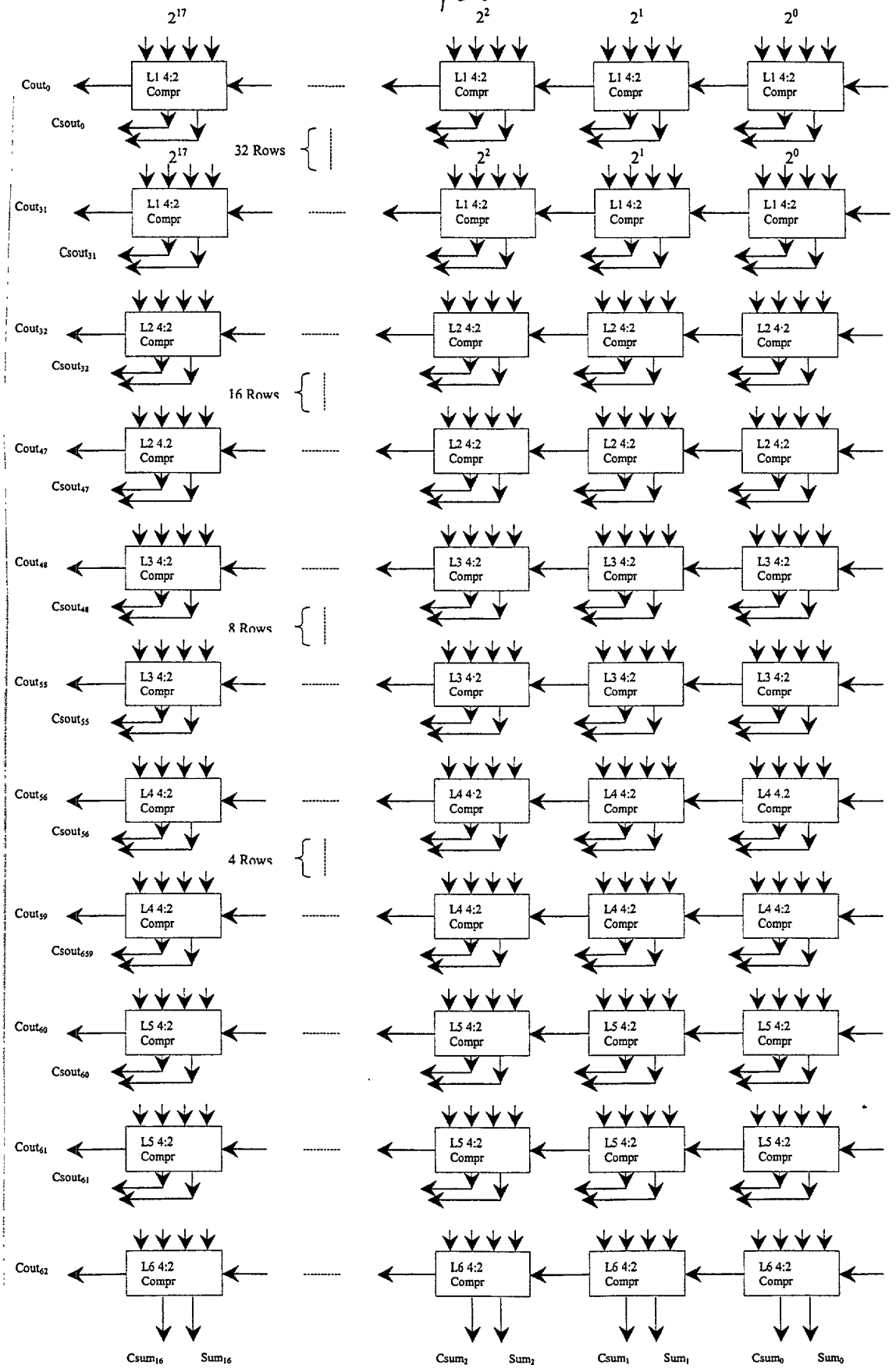


FIG. 20

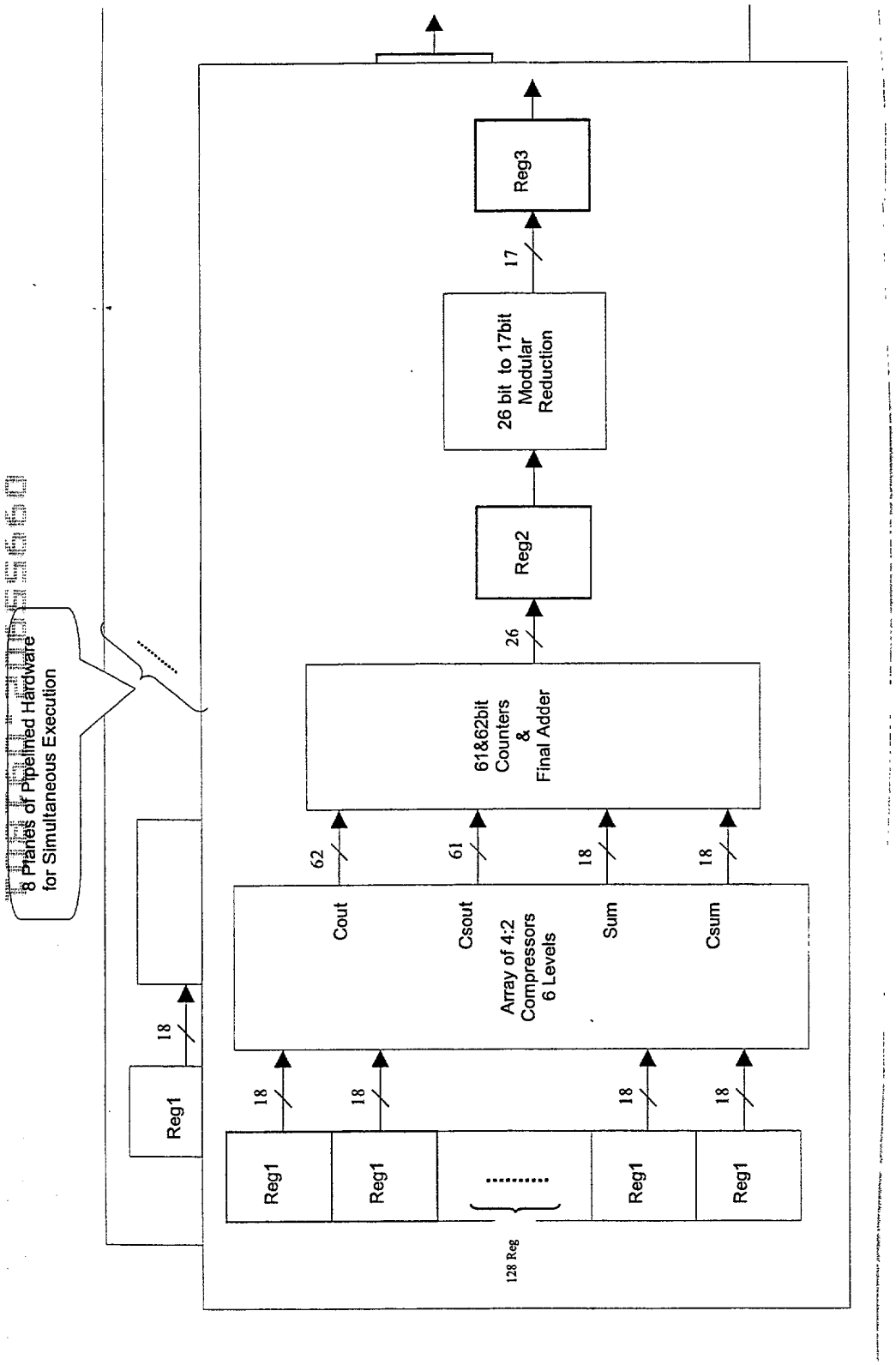

8 Planes of Pipelined Hardware for Simultaneous Execution
Reg1
18
Reg1
Reg1
Reg1
Reg1
18
18
18
18
128 Reg
Array of 4:2 Compressors 6 Levels
Cout
Csout
Sum
Csum
62
61
18
18
61&62bit Counters & Final Adder
26
Reg2
26 bit to 17bit Modular Reduction
17
Reg3

FIG. 21

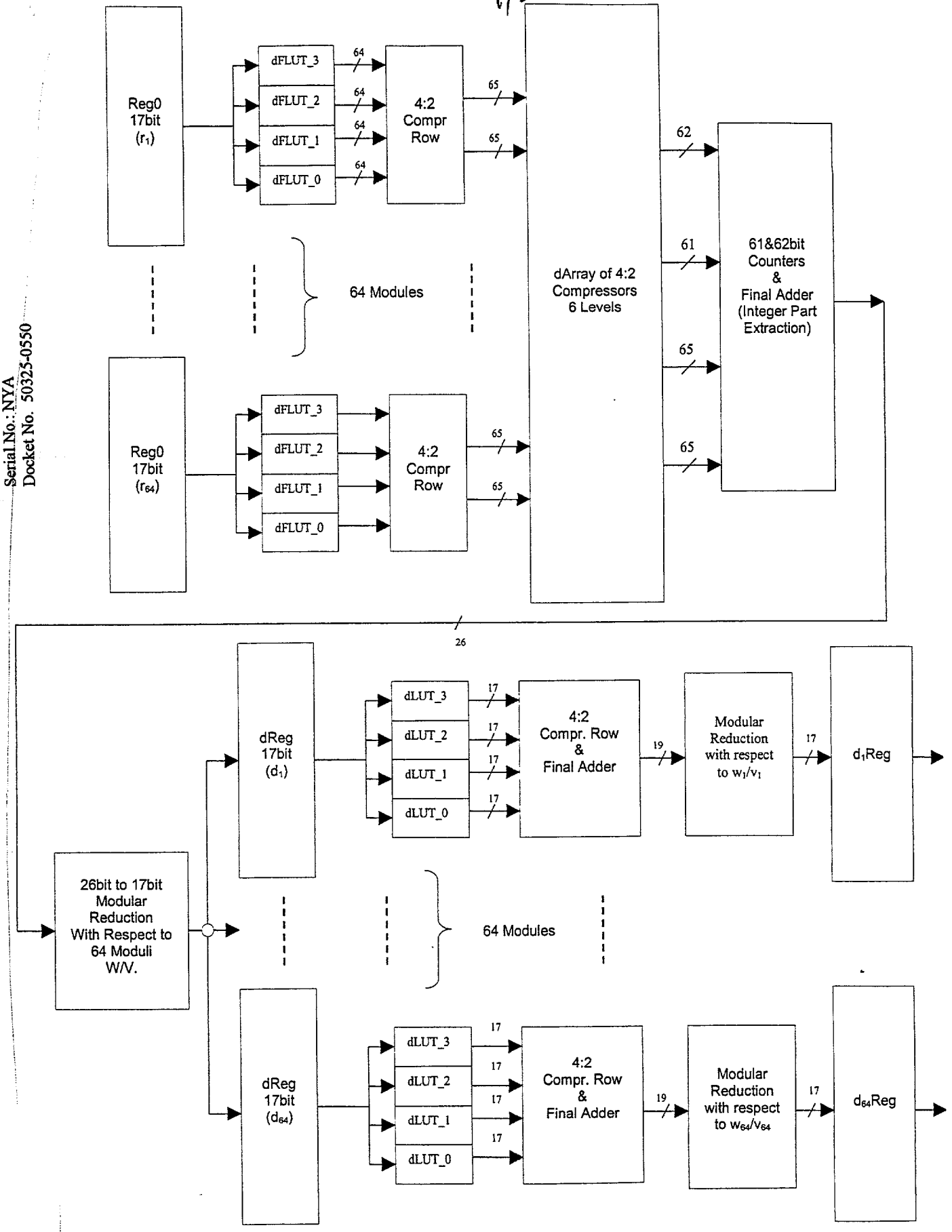
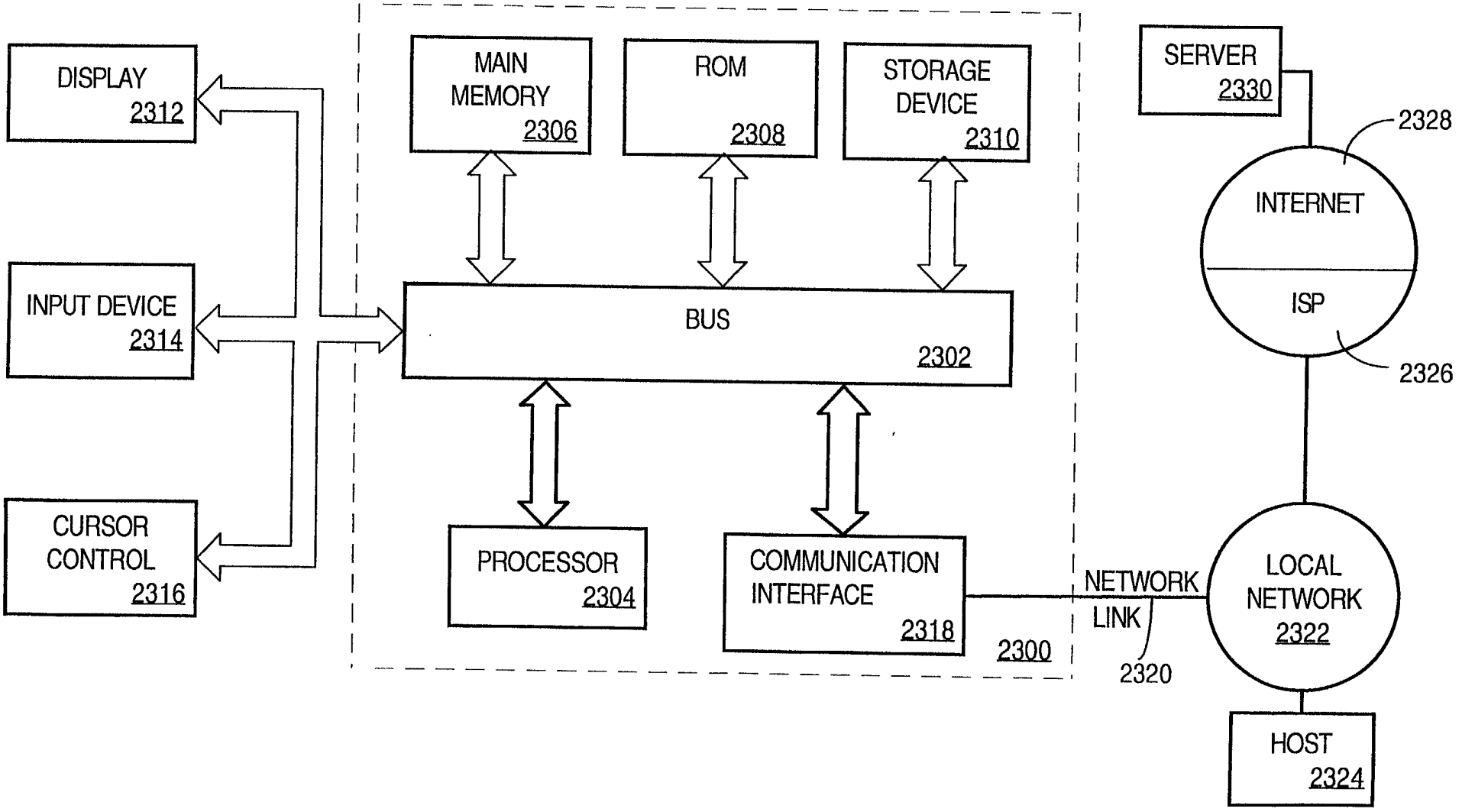


FIG. 22

FIG. 23


DISPLAY
2312
INPUT DEVICE
2314
CURSOR CONTROL
2316
MAIN MEMORY
2306
ROM
2308
STORAGE DEVICE
2310
BUS
2302
PROCESSOR
2304
COMMUNICATION INTERFACE
2318
2300
NETWORK LINK
2320
SERVER
2330
2328
INTERNET
ISP
2326
LOCAL NETWORK
2322
HOST
2324